

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY

**As rescanning documents *will not* correct
images, please do not report the images to the
Image Problem Mailbox.**

This Page Blank (isnto)

BUNDESREPUBLIK DEUTSCHLAND

09 E806435



REC'D	06 DEC 1999
WIPO	PCT

Bescheinigung

Die Siemens Aktiengesellschaft in München/Deutschland hat eine Patentanmeldung unter der Bezeichnung

"Verfahren und Anordnung zur Aktualisierung eines Paßwortes"

am 30. September 1998 beim Deutschen Patent- und Markenamt eingereicht.

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

Die Anmeldung hat im Deutschen Patent- und Markenamt vorläufig das Symbol H 04 L 12/22 der Internationalen Patentklassifikation erhalten.

München, den 2. November 1999

Deutsches Patent- und Markenamt

Der Präsident

im Auftrag

zeichen: 198 45 055.9

Sieci

PRIORITY DOCUMENT
 SUBMITTED OR TRANSMITTED IN
 COMPLIANCE WITH
 RULE 17.1(a) OR (b)

This Page Blank (uspto)

**Beschreibung****Verfahren und Anordnung zur Aktualisierung eines Paßwortes**

5 Die Erfindung betrifft ein Verfahren und eine Anordnung zur Aktualisierung eines Paßwortes.

Aus [1] sind ein solches Verfahren und eine solche Anordnung bekannt.

10 Bei einer solchen Anordnung ist für den Fall, daß ein Benutzer diese Anordnung benutzen will, vorgesehen, daß von dem Benutzer eine Eingabe eines Paßwortes in die Anordnung gefordert wird. Nach Eingabe des Paßwortes durch den Benutzer wird
15 von der Anordnung anhand einer Datenbank überprüft, ob eine eingegebene Paßwortangabe für den Benutzer ein gültiges Paßwort ist oder nicht.

20 In der Datenbank der Anordnung ist eine Liste mit zulässigen Benutzern der Anordnung gespeichert. Jedem Benutzer ist jeweils ein Paßwort zugeordnet, welches gespeichert ist und mit dem das eingegebene Paßwort verglichen wird. Jedem Paßwort ist ferner eine Zeitangabe zugeordnet. Mit der Zeitangabe wird angegeben, für welchen Zeitraum das Paßwort gültig sein soll. Ist der Zeitraum abgelaufen, so wird das gespeicherte Paßwort ungültig und der Benutzer wird zu einer Aktualisierung des Paßwortes aufgefordert, wenn er die Benutzung der Anordnung aufnehmen will.

30 Auf diese Weise wird eine gewisse, von dem jeweiligen Zeitraum abhängige Aktualität des jeweiligen Paßwortes erreicht, wodurch ein höherer Sicherheitsgrad für die Anordnung hinsichtlich eines Mißbrauchs bzw. eines unbefugten Ermittelns eines Paßworts gewährleistet wird. Ferner ist aus [1] bekannt, daß die Paßwortangabe in der Datenbank in kryptierter Form (verschlüsselt oder gebildet unter Verwendung einer Einweg-Hashfunktion) abgelegt werden kann. Aus [1] ist weiterhin

bekannt, daß die Paßwortangabe kryptiert über eine Kommunikationsverbindung transportiert werden kann. Ein Beispiel dafür ist das Domain Logon bei Windows NT. Der Zeitpunkt des Paßwortwechsels ist jedoch auf den Zeitpunkt der Login-Prozedur

5 beschränkt.

Aus [2] ist ein Kommunikationsstandard, der H.235-Standard, bekannt, in dem Rahmenbedingungen, insbesondere Formate von Nachrichten, die zwischen miteinander verbundenen Rechnern im

10 Rahmen einer multimedialen Kommunikation ausgetauscht werden können.

Die Rechner können logisch oder fest miteinander verbunden sein.

15 Ein Nachteil der aus [2] bekannten Verfahren ist insbesondere darin zu sehen, daß lediglich statische Paßworte für einen Benutzer eingesetzt werden können, wodurch die Wahrscheinlichkeit relativ hoch ist, daß in den Rechnern gespeicherte

20 Paßworte irgendwann von einem unbefugten Dritten, einem Angreifer, ermittelt und mißbraucht werden können, wodurch die Sicherheit der einzelnen Rechner nicht mehr gewährleistet ist.

25 Aus [3] ist ein weiterer Kommunikationsstandard, der H.225-Standard, bekannt.

Aus [4] ist die sogenannte Abstract Syntax Notation 1 (ASN.1) beschrieben, die zur Definition des Formats einer Nachricht

30 verwendet wird, die zur Definition des Formats einer Nachricht im Sinne der aus [2] und [3] bekannten Standards verwendet wird.

35 Eine Übersicht über Protokolle zur Aktualisierung kryptografischer Schlüssel ist in [5] zu finden.

Insbesondere bei einem großen Kommunikationsnetz mit einer Vielzahl miteinander verbundenen Rechnern, beispielsweise dem Internet, stellt die oben beschriebene Situation ein hohes Risiko dar.

5

Somit liegt der Erfindung das Problem zugrunde, ein Verfahren und eine Anordnung zur Aktualisierung eines Paßwortes zwischen zwei miteinander verbundenen Rechnern anzugeben.

10 Das Problem wird durch die Anordnung sowie das Verfahren mit den Merkmalen gemäß den unabhängigen Ansprüchen gelöst.

Ein Verfahren zur Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner, weist folgende 15 Schritte auf:

- a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
- b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
- c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
- d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
- e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paßworts gefordert wird, und
- f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

30

35

Eine Anordnung weist mindestens einen ersten Rechner und mindestens einen zweiten Rechner auf zur Aktualisierung eines Paßwortes zwischen den Rechnern,

5 wobei der erste Rechner und der zweite Rechner jeweils einen Prozessor aufweisen, die derart eingerichtet sind, daß fol-

gende Schritte durchführbar sind:

a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,

10 b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,

c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,

15 d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,

e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paßworts gefordert wird, und

20 f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

Durch die Erfindung wird eine Aktualisierung eines Paßwortes zwischen zwei Rechnern während einer zwischen den beiden

30 Rechnern bestehenden Kommunikationsverbindung möglich. Der zweite Rechner kann den ersten Rechner anschaulich dazu zwingen, daß der erste Rechner das Paßwort zu aktualisieren hat, wenn der erste Rechner einen Dienst von dem zweiten Rechner anfordert. Damit gewährleistet der zweite Rechner die Aktualität der Paßworte, wodurch die Sicherheit der Kommunikation zwischen den Rechnern erhöht wird.

Bevorzugte Weiterbildungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Die im weiteren beschriebenen Weiterbildungen gelten sowohl für das Verfahren als auch die Anordnung, wobei bei der Weiterbildung der Anordnung jeweils die Prozessoren der Rechner derart eingerichtet sind, daß die Weiterbildung realisierbar ist.

10 Die Bildung des aktualisierten Paßwortes erfolgt in einer Weiterbildung auf folgende Weise:

- a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthalten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,
- 15 b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
- c) der zweite Rechner speichert das aktualisierte Paßwort.

20 Der zweite Rechner kann eine Bestätigungs Nachricht senden, mit der der Einsatz des aktualisierten Paßwortes im Rahmen der Kommunikationsverbindung bestätigt wird.

Zu Beginn des Verfahrens wird vorzugsweise der erste Rechner durch den zweiten Rechner authentifiziert unter Verwendung einer in der Dienstanforderungsnachricht enthaltenen Authentifikationsangabe des ersten Rechners. Damit wird das Sicherheitsniveau der jeweiligen Kommunikationsverbindung erhöht.

30 Die Überprüfung, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist, erfolgt in einer weiteren Ausgestaltung anhand einer Kontrolldatenbank, in der für den ersten Rechner angegeben ist, ob zuvor schon von dem zweiten Rechner eine Aktualisierungsnachricht 35 an den ersten Rechner gesendet worden ist. Durch diese Vereinfachung wird das Verfahren schneller durchführbar, da eine

erhebliche Rechenzeiteinsparung im Rahmen der Überprüfung erreicht wird.

In der Dienstanforderungsnachricht ist bevorzugt eine Angabe 5 enthalten zur Integritätssicherung der Dienstanforderungsnachricht, mit welcher Angabe von dem zweiten Rechner die empfangene Dienstanforderungsnachricht auf ihre Integrität hin überprüft wird. Nur für den Fall, daß die Integrität der Dienstanforderungsnachricht gewährleistet ist, wird das Verfahren durchgeführt; sonst wird der angeforderte Dienst zurückgewiesen. Damit wird das Sicherheitsniveau der jeweiligen Kommunikationsverbindung weiter erhöht.

In der Paßwortnachricht ist das aktualisierte Paßwort bevorzugt verschlüsselt enthalten, wobei der Schlüssel zur Verschlüsselung des aktualisierten Paßwortes abhängig von dem Paßwort gebildet wird. Durch diese Weiterbildung wird ein Zusammenhang zwischen dem „alten“ Paßwort und dem aktualisierten Paßwort geschaffen, womit nur der Besitzer des Paßwortes 20 das aktualisierte Paßwort überhaupt ermitteln kann. Damit wird der Schutz des aktualisierten Paßwortes bei dessen Übertragung verbessert.

Der Schlüssel wird bevorzugt durch mehrfache Aneinanderreihung des Paßwortes gebildet.

Es sind vorzugsweise mehrere erste Rechner vorgesehen, die jeweils ein Paßwort gemeinsam mit dem zweiten Rechner besitzen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen ersten Rechner und dem zweiten Rechner. Damit ist die Erfindung sehr gut einsetzbar in einem großen Kommunikationsnetz, in dem ein Server, der zweite Rechner, mehreren Clients, den ersten Rechnern, Dienste über das Kommunikationsnetz anbietet.

35

Ferner können mehrere zweite Rechnern vorgesehen sein, die jeweils ein Paßwort gemeinsam mit jedem ersten Rechner besit-

zen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen zweiten Rechner und dem jeweiligen zweiten Rechner.

5 Ein Ausführungsbeispiel der Erfindung ist in den Figuren dargestellt und wird im weiteren näher erläutert:

Es zeigen

10 Figur 1 ein Ablaufdiagramm, in dem die Verfahrensschritte des Ausführungsbeispiels dargestellt sind;

Figur 2 eine Skizze, in der Rechner dargestellt sind, die über ein Kommunikationsnetz miteinander verbunden sind.

15

Fig.2 zeigt einen ersten Rechner 200 mit einem Speicher 202 und einem Prozessor 203, die jeweils über einen Bus 204 miteinander und mit einer Eingangs-/Ausgangsschnittstelle 201 verbunden sind.

Über die Eingangs-/Ausgangsschnittstelle 201 ist der erste Rechner 200 mit einem Bildschirm 205, einer Tastatur 206 sowie einer Computermaus 207 verbunden.

Ferner ist der erste Rechner 200 über ein Kommunikationsnetz 260, in dem Beispiel ein ISDN-Netz (Integrated Services Digital Network) mit weiteren Rechnern 210, 220, 230, 240 und 250 verbunden.

30

In dem ersten Rechner 200 ist eine Datenbank 208 gespeichert.

Die weiteren Rechner 210, 220, 230, 240 und 250 weisen jeweils ebenfalls einen Prozessor 213, 223, 233, 243 und 253 sowie jeweils einen Speicher 212, 222, 232, 242 und 252 auf. Jeweils der Prozessor 213, 223, 233, 243 und 253 und der Speicher 212, 222, 232, 242 und 252 sind über jeweils einen

5 Bus 214, 224, 234, 244 und 254 über eine Eingangs-/Ausgangsschnittstelle 211, 221, 231, 241 und 251 mit dem Kommunikationsnetz 260 verbunden. Ferner sind die weiteren Rechner 210, 220, 230, 240 und 250 jeweils mit einem Bildschirm 215, 225, 235, 245 und 255 sowie einer Tastatur 216, 226, 236, 246 und 256 sowie einer Computermaus 217, 227, 237, 247 und 257 verbunden.

10 Zwischen den Rechnern 200, 210, 220, 230, 240 und 250 erfolgt die Kommunikation, d.h. ein gesicherter Austausch multimedia-
15 ler Daten, gemäß dem H.235-Standard, wie in [2] beschrieben.

15 Der erste Rechner 200 ist als ein Server ausgestaltet und stellt den weiteren Rechnern 210, 220, 230, 240 und 250 ver-
20 schiedene Dienste zur Verfügung.

20 Im weiteren wird angenommen, daß ein zweiter Rechner 210 einen Dienst von dem ersten Rechner 200 in Anspruch nehmen will.

25 Zu Beginn des Verfahrens wird eine Kommunikationsverbindung zwischen dem zweiten Rechner 210 und dem ersten Rechner 200 gemäß den in [2] und [3] beschriebenen Verfahren aufgebaut. Nach erfolgter Initialisierung der Kommunikationsverbindung besteht zwischen dem zweiten Rechner 210 und dem ersten Rechner 200 eine logische Verbindung, d.h. der Kommunikationsver-
30 bindung ist ein logischer Kanal zugeordnet, der eindeutig identifizierbar ist. Über den logischen Kanal werden zwischen den Rechnern 200, 210, 220, 230, 240, 250 Nachrichten 270, 280 ausgetauscht.

35 Ist die Kommunikationsverbindung aufgebaut, kann durch den zweiten Rechner 210 von dem ersten Rechner 200 ein Dienst in Anspruch genommen, in diesem Fall eine Datenbankabfrage von einer in dem ersten Rechner 200 gespeicherten Datenbank 208.

Im weiteren wird das Verfahren beschrieben, das durchgeführt wird, wenn der zweite Rechner 210 von dem ersten Rechner 200 Daten aus dessen Datenbank 208 ermitteln möchte.

5 Die gewünschten Kriterien für die Datenbankabfrage werden von
einem Benutzer des zweiten Rechners 210 in den zweiten Rech-
ner 210 eingegeben. Von dem zweiten Rechner 210 wird eine
Dienstanforderungsnachricht 101 gebildet (Schritt 100), in
der die Kriterien für die Datenbankabfrage enthalten sind
10 (vgl. Fig.1).

Ferner sind in der Dienstanforderungsnachricht 101 folgende
Größen enthalten:

15 - eine Authentifikationsangabe (Authentication Token), mit
der eine Authentifikation des zweiten Rechners 210 durch den
ersten Rechner 200 möglich ist; die Authentifikationsangabe
erlaubt die Darstellung des Paßwortes in verschiedener Form
(beispielsweise verschlüsselt oder gebildet unter Verwendung
einer Einweg-Hashfunktion als Einweg-Hashwert);
20 - eine H.235-Adresse, mit der der erste Rechner 200 eindeutig
identifiziert wird;
- eine Paßwortangabe PW des Benutzers des zweiten Rechners
210.

30 In dem ersten Rechner 200 ist für jeden weiteren Rechner 210,
220, 230, 240 und 250 ein dem jeweiligen Rechner 210, 220,
230, 240 und 250 zugeordnetes Paßwort gespeichert. Ist in ei-
ner Dienstanforderungsnachricht 101, die von einem weiteren
Rechner 210, 220, 230, 240 und 250 gebildet wird, eine Paß-
wortangabe enthalten, die gleich dem gespeicherten Paßwort
für den weiteren Rechner 210, 220, 230, 240 und 250 ist, so
wird der angeforderte Dienst dem Benutzer gewährt, d.h. von
dem ersten Rechner 200 ausgeführt.

35 Dem Paßwort ist jeweils eine erste Zeitangabe t1 zugeordnet,
mit der angegeben wird, zu welchem Zeitpunkt das Paßwort ge-
bildet worden ist. Ferner ist dem Paßwort jeweils eine zweite

10

Zeitangabe t_2 zugeordnet, mit der angegeben wird, für welchen Zeitraum das Paßwort gültig ist.

5 Die Dienstanforderungsnachricht 101 wird von dem zweiten Rechner 210 an den ersten Rechner 200 übertragen (Schritt 102).

10 Nach Empfang der Dienstanforderungsnachricht 101 in dem ersten Rechner 200 (Schritt 103) wird der zweite Rechner 210 unter Verwendung der Authentifikationsangabe in der Dienstanforderungsnachricht 101 authentifiziert (Schritt 104).

15 Nach positiver Authentifikation des zweiten Rechners 210 wird in einem weiteren Schritt (Schritt 105) die Paßwortangabe PW aus der Authentifikationsangabe der Dienstanforderungsnachricht 101 ermittelt und die Paßwortangabe wird mit dem in dem ersten Rechner 200 gespeicherten Paßwort, welches dem zweiten Rechner 200 zugeordnet ist, verglichen (Schritt 106).

20 Bei negativer Authentifikation wird die Dienstanforderungsnachricht 101 verworfen (Schritt 110) und der angeforderte Dienst wird nicht ausgeführt.

25 Stimmen die Paßwortangabe PW und das dem zweiten Rechner 200 zugeordnete Paßwort überein, so wird überprüft, ob das Paßwort gültig ist (Schritt 107). Dies erfolgt in der Weise, daß eine aktuelle Zeit t_3 , zu der die Dienstanforderungsnachricht 101 von dem ersten Rechner 200 empfangen worden ist, ermittelt wird.

30 Stimmen die Paßwortangabe PW und das dem zweiten Rechner 200 zugeordnete Paßwort überein, so wird die Dienstanforderungsnachricht 101 verworfen (Schritt 115) und der angeforderte Dienst wird nicht ausgeführt.

Es wird überprüft, ob die aktuelle Zeit t_3 kleiner oder gleich ist der Summe aus der ersten Zeitangabe t_1 und der zweiten Zeitangabe t_2 , also ob gilt:

5 $t_3 \leq t_1 + t_2.$ (1)

Ist Vorschrift (1) erfüllt, so bedeutet dies, daß die Paßwortangabe dem Paßwort entspricht und das Paßwort noch gültig ist.

10 In diesem Fall wird der mit der Dienstanforderung 101 angeforderte Dienst, also die Datenbankabfrage von dem ersten Rechner 200 durchgeführt (Schritt 108) und das Ergebnis der Datenbankabfrage wird in einer gebildeten Ergebnisnachricht 116 (Schritt 109) an den zweiten Rechner 210 übertragen (Schritt 110), in dem das Ergebnis der Datenbankabfrage weiterverarbeitet wird (Schritt 111).

20 Ist Vorschrift (1) nicht erfüllt, so bedeutet dies, daß zwar der zweite Rechner 210 aufgrund der erfolgten Authentifikation grundsätzlich zur Anforderung des Dienstes berechtigt ist, das dem zweiten Rechner 210 zugeordnete Paßwort nicht mehr gültig ist.

25 In einem weiteren Schritt (Schritt 120) wird bei ungültigem Paßwort von dem ersten Rechner 200 eine Aktualisierungsnachricht 121 gebildet und an den zweiten Rechner 210 gesendet (Schritt 122), mit der eine Aktualisierung des Paßworts gefordert wird. Ferner wird von dem ersten Rechner 200 in einer Kontrolldatenbank ein Bit (Kontrollwert) auf einen ersten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort ungültig ist und die entsprechende Aktualisierungsnachricht 121 an den zweiten Rechner 210 gesendet worden ist.

35 Nach Empfang der Aktualisierungsnachricht 121 (Schritt 123) wird von dem zweiten Rechner ein aktualisiertes Paßwort aPW gebildet (Schritt 124).

Hält sich der zweite Rechner 210 nicht an die vorgeschriebene Prozedur und generiert erneut eine Dienstanforderung, ohne das Paßwort zu ändern, so kann der erste Rechner 200 dies

5 nach der Authentifikation des zweiten Rechners 210 und dem Überprüfen des Kontrollwertes feststellen. Ist der Kontrollwert auf den ersten Wert gesetzt, so kann das Verfahren beendet werden (Schritt 131).

10 Das aktualisierte Paßwort aPW wird symmetrisch gemäß dem Data Encryption Standard (DES) verschlüsselt. Als Schlüssel wird das Paßwort PW, welches auch in dem zweiten Rechner 210 bekannt und gespeichert ist, zur Verschlüsselung des aktualisierten Paßworts aPW verwendet.

15 Das verschlüsselte aktualisierte Paßwort aPW wird in einer von dem zweiten Rechner 210 gebildeten Paßwortnachricht 125 (Schritt 126) an den ersten Rechner übertragen (Schritt 127).

20 In der Paßwortnachricht 125 ist eine Integritätsangabe enthalten, mit der die Integrität der Paßwortnachricht 125 überprüft werden kann.

25 Nach Empfang der Paßwortnachricht 125 (Schritt 128) wird die Integrität der Paßwortnachricht 125 überprüft (Schritt 129).

Bei negativer Integritätsprüfung wird die Paßwortnachricht 125 verworfen (Schritt 130) und das Verfahren beendet (Schritt 131).

30 Bei positiver Integritätsprüfung wird von dem ersten Rechner 200 das verschlüsselte aktualisierte Paßwort aPW ermittelt (Schritt 132) und das aktualisierte Paßwort aPW wird entschlüsselt (Schritt 133).

35 Das ermittelte aktualisierte Paßwort aPW wird in einem weiteren Schritt als neues Paßwort für den zweiten Rechner 210 ge-

speichert (Schritt 134). Ferner wird von dem ersten Rechner 200 in der Kontrolldatenbank der entsprechende Kontrollwert auf einen zweiten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort gültig ist.

5

Anschließend wird von dem ersten Rechner 200 eine Bestätigungs-nachricht 135 gebildet (Schritt 136) und an den zweiten Rechner 210 übertragen (Schritt 137) und von dem zweiten Rechner 210 empfangen (Schritt 138). Mit der Bestätigungs-nachricht 135 wird dem zweiten Rechner 210 der weitere Einsatz des aktualisierten Paßwortes aPW im Rahmen der Kommunikationsverbindung bestätigt.

10 Weiterhin wird von dem ersten Rechner 200 der Dienst erbracht (Schritt 108), die Ergebnisnachricht 116 gebildet (Schritt 109) und die Ergebnisnachricht 116 an den zweiten Rechner 210 übertragen (Schritt 110). In dem zweiten Rechner 210 wird die Ergebnisnachricht 116 weiterverarbeitet (Schritt 111).

20

Ferner wird von dem ersten Rechner 200 in der Kontrolldatenbank das entsprechende Bit auf einen zweiten Wert gesetzt, mit dem angegeben wird, daß das jeweilige Paßwort gültig ist.

25

Bei einer weiteren empfangenen Dienstanforderungsnachricht wird jeweils nach deren Empfang von dem ersten Rechner 200 anhand der Kontrolldatenbank überprüft, ob das jeweilige Paßwort gültig ist oder nicht. Auf diese Weise wird eine sehr schnelle Prüfung des Paßwortes erreicht.

30

Die im Rahmen dieses Verfahrens verwendeten Nachrichten sind gemäß dem H.225.0-Standard, wie er in [3] beschrieben ist, codiert.

35

Zur Definition des im weiteren beschriebenen Formats der einzelnen Nachrichten wird die in [4] beschriebene Abstract Syntax Notation 1 (ASN.1) verwendet.

Die Nachrichten werden als eine in [3] vorgesehene NonStandardMessage codiert, wie im folgenden beschrieben:

```
5  NonStandardMessage ::= SEQUENCE
{
    requestSeqNum           RequestSeqNum,
    nonStandardData         NonStandardParameter,
    ...
    tokens                  SEQUENCE OF ClearToken OPTIONAL,
    cryptoTokens            SEQUENCE OF CryptoH323Token OPTIONAL,
    integrityCheckValue    ICV OPTIONAL
}

10
15  NonStandardParameter ::= SEQUENCE
{
    nonStandardIdentifier  NonStandardIdentifier,
    data                   OCTET STRING
20 }

25
30  NonStandardIdentifier ::= CHOICE
{
    object                 OBJECT IDENTIFIER,
    h221NonStandard        H221NonStandard,
    ...
}

35
40  data ::= SEQUENCE
{
    alias                  GatekeeperIdentifier,
    confirm                boolean,
    ...
    -- optionally for the provision of integrity
    rejectReason           PWUpdateRejectReason OPTIONAL,
    hash_algorithm          NonIsoIntegrityMechanism OPTIONAL,
    token                  HASHED OPTIONAL,
    ...
    -- < alias, confirmation, new password>
}

45  PWUpdateRejectReason ::= CHOICE
{
    notregistered          NULL, -- keep the old password
    pw_wrong               NULL, -- keep the old password
    pw_old                NULL, -- keep the old password
    ...
}

50 }
```

```

NonIsoIntegrityMechanism ::= CHOICE
{   -- HMAC mechanism used, no truncation, tagging may bei dem
necessary!
    HMAC-MD5           NULL,
5    HMAC-iso10118-2-s EncryptIntAlg,
    -- according to ISO/IEC 10118-2 using
    -- EncryptIntAlg as core block encryption algorithm
    -- (short MAC)
    HMAC-iso10118-2-1 EncryptIntAlg,
10   -- according to ISO/IEC 10118-2 using
    -- EncryptIntAlg as core block encryption algorithm
    -- (long MAC)
    HMAC-iso10118-3  OBJECT IDENTIFIER,
    -- according to ISO/IEC 10118-3 using
    -- OID as hash function (OID is SHA-1, RIPE-MD160,
    -- RIPE-MD128)
    ...
15
}

EncryptIntAlg ::= CHOICE
{   -- core encryption algorithms for RAS message integrity
    nonStandard   NonStandardParameter,
    isoAlgorithm  OBJECT IDENTIFIER,      -- defined in
25  ISO/IEC 9979
    ...
}

AliasAddress ::= CHOICE
{
    e164      IA5String (SIZE (1..128)) (FROM („0123456789#*,“)),
    h323-ID   BMPString (SIZE (1..256)),
    -- Basic ISO/IEC 10646-1 (Unicode)
35    ....
    url-ID    IA5String (SIZE (1..512)),
    -- URL style address
    transportID TransportAddress,
    email-ID   IA5String (SIZE (1..512)),
    -- rfc822-compliant email address
40    partyNumber PartyNumber
}

```

Im weiteren sind einige Alternativen zu dem oben beschriebenen
45 Ausführungsbeispiel dargestellt:

Die Art der Integritätssicherung ist grundsätzlich beliebig,
ebenso wie der Verschlüsselungsalgorithmus zur Verschlüsse-
lung des aktualisierten Paßwortes.

50

Die Realisierung der Nachrichten als Non Standard Messages
bzw. Non Standard Data Field ist nicht zwingend notwendig.
Die Darstellung der Nachrichten lässt sich auch über neu zu

definierende Nachrichten oder Protokollfelder in den aus [2] und [3] bekannten Standards realisieren.

Auch sind das Verfahren und die Anordnung nicht auf die aus 5 [2] und [3] bekannten Standards beschränkt.

Die Bildung der Dienstanforderungsnachricht und/oder der Aktualisierungsnachricht und/oder der Paßwortnachricht und/oder der Bestätigungsrichtung können separat als eigenständige 10 Nachrichten erfolgen und zwischen den beteiligten Rechnern separat übertragen werden. Es ist ferner in einer Variante möglich, die jeweilige Nachricht gemäß dem Prinzip des sogenannten "Piggybacks" gemeinsam mit anderen Nachrichten zwischen den beteiligten Rechnern zu übertragen.

15 Auch kann der zweite Rechner durch Senden einer Aktualisierungsanforderung an den zweiten Rechner die Bildung eines neuen Paßwortes beim zweiten Rechner anfordern. Analog zuden obigen Ausführungen kann der zweite Rechner mit Hilfe einer 20 bei ihm gespeicherten Kontrolldatenbank und dem entsprechenden Kontrollwert überprüfen, ob der erste Rechner seiner Auflorderung zum Paßwortwechsel nachgekommen ist. Im negativen Fall kann der zweite Rechner die Kommunikation abbrechen und das Verfahren beenden.

In diesem Dokument sind folgende Veröffentlichungen zitiert:

5 [1] Microsoft Developper Network Library, Questions 151082
S7D6D, S7590, S759E, S5970, Microsoft Press, Juli 1998,
erhältlich am 29. September 1998 im Internet unter der
folgenden Adresse:

<http://msdn.microsoft.com/developer/>

10 [2] International Telecommunication Union, Draft ITU-T Recom-
mendation H.235, Line Transmission of Non-Telephone Si-
gnals, Security and Encryption for H Series (H.323 and
Other H.245 Based) Multimedia Terminals), Version 1, Ka-
pitel 10.3.2, September 1997

15 [3] International Telecommunication Union, Draft ITU-T Recom-
mendation H.225.0, Line Transmission of Non-Telephone Si-
gnals, Call Signaling Protocols and Media Stream Packe-
tization for Packet Based Multimedia Communiacations Sy-
stems, Version 2, Kapitel 7.6 und 7.16, March 1997

20 [4] International Telecommunication Union, X.680 - X.683: OSI
NETWORKING AND SYSTEM ASPECTS - ABSTRACT SYNTAX NOTATION
ONE (ASN.1), July 1994

[5] A. J. Menezes et al, Handbook of Applied Cryptography,
CRC Press, New York, S. 497 - 504, 1997, ISBN 0-8493-
8523-7

Patentansprüche

1. Verfahren zur Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner,

5 a) bei dem der zweite Rechner im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht empfängt, wobei die Dienstanforderungsnachricht das Paßwort aufweist,

10 b) bei dem mit der Dienstanforderungsnachricht von dem ersten Rechner die Erbringung eines Dienstes angefordert wird,

15 c) bei dem der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,

20 d) bei dem für den Fall, daß das Paßwort gültig ist, der Dienst erbracht wird,

25 e) bei dem für den Fall, daß das Paßwort ungültig ist, von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet wird, mit der eine Aktualisierung des Paßworts gefordert wird, und

30 f) bei dem von dem ersten Rechner und/oder dem zweiten Rechner ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

25

2. Verfahren nach Anspruch 1,

bei dem die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:

30 a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthalten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,

35 b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,

40 c) der zweite Rechner speichert das aktualisierte Paßwort.

3. Verfahren nach Anspruch 2,

bei dem der zweite Rechner eine Bestätigungs Nachricht sendet, mit der der Einsatz des aktualisierten Paßwortes im Rahmen der Kommunikationsverbindung bestätigt wird.

5 4. Verfahren nach einem der Ansprüche 1 bis 3,
bei dem zu Beginn des Verfahrens der erste Rechner durch den zweiten Rechner authentifiziert wird unter Verwendung einer in der Dienstanforderungsnachricht enthaltenen Authentifikationsangabe des ersten Rechners.

10

5. Verfahren nach einem der Ansprüche 1 bis 4,
bei dem die Überprüfung, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist, anhand einer Kontrolldatenbank erfolgt, in der für den ersten Rechner angegeben ist, ob zuvor schon von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet worden ist.

6. Verfahren nach einem der Ansprüche 1 bis 5,
20 a) bei dem in der Dienstanforderungsnachricht eine Angabe enthalten zur Integritätssicherung der Dienstanforderungsnachricht,
b) bei dem von dem zweiten Rechner die empfangene Dienstanforderungsnachricht auf ihre Integrität überprüft wird,
c) bei dem nur für den Fall, daß die Integrität der Dienstanforderungsnachricht gewährleistet ist, das Verfahren durchgeführt wird, und
d) sonst der angeforderte Dienst zurückgewiesen wird.

30 7. Verfahren nach einem der Ansprüche 2 bis 6,
bei dem in der Paßwortnachricht das aktualisierte Paßwort verschlüsselt enthalten ist, wobei der Schlüssel zur Verschlüsselung des aktualisierten Paßwortes abhängig von dem Paßwort gebildet wird.

35

8. Verfahren nach Anspruch 7,

bei dem der Schlüssel durch mehrfache Aneinanderreihung des Paßwortes gebildet wird.

9. Anordnung mit mindestens einem ersten Rechner und mindestens einem zweiten Rechner zur Aktualisierung eines Paßwortes zwischen den Rechnern,

wobei der erste Rechner und der zweite Rechner jeweils einen Prozessor aufweisen, die derart eingerichtet sind, daß folgende Schritte durchführbar sind:

- 10 a) der zweite Rechner empfängt im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht, wobei die Dienstanforderungsnachricht das Paßwort aufweist,
- 15 b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,
- c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,
- 20 d) für den Fall, daß das Paßwort gültig ist, wird der Dienst erbracht,
- e) für den Fall, daß das Paßwort ungültig ist, wird von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet, mit der eine Aktualisierung des Paßworts gefordert wird, und
- 25 f) von dem ersten Rechner und/oder dem zweiten Rechner wird ein aktualisiertes Paßwort gebildet, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

30

10. Anordnung nach Anspruch 9,

bei der die Prozessoren derart eingerichtet sind, daß die Bildung des aktualisierten Paßwortes auf folgende Weise erfolgt:

- 35 a) der erste Rechner sendet eine Paßwortnachricht zu dem zweiten Rechner, in der das aktualisierte Paßwort enthal-

ten ist in einer Weise, daß das aktualisierte Paßwort nur unter Verwendung des Paßwortes ermittelt werden kann,

5 b) der zweite Rechner ermittelt unter Verwendung des Paßwortes das aktualisierte Paßwort aus der Paßwortnachricht,
5 c) der zweite Rechner speichert das aktualisierte Paßwort.

11. Anordnung nach Anspruch 9 oder 10,

mit mehreren ersten Rechnern, die jeweils ein Paßwort gemeinsam mit dem zweiten Rechner besitzen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen ersten Rechner und dem zweiten Rechner.

10 12. Anordnung nach einem der Ansprüche 9 bis 11,

mit mehreren zweiten Rechnern, die jeweils ein Paßwort gemeinsam mit jedem ersten Rechner besitzen, wobei das Paßwort jeweils eindeutig ist für die Kommunikationsverbindung zwischen dem jeweiligen zweiten Rechner und dem jeweiligen zweiten Rechner.



Zusammenfassung**Verfahren und Anordnung zur Aktualisierung eines Paßwortes**

5 Es erfolgt eine Aktualisierung eines Paßwortes zwischen einem ersten Rechner und einem zweiten Rechner, wobei

10 a) der zweite Rechner im Rahmen einer zwischen dem ersten Rechner und dem zweiten Rechner bestehenden Kommunikationsverbindung eine von dem ersten Rechner gesendete Dienstanforderungsnachricht empfängt, wobei die Dienstanforderungsnachricht das Paßwort aufweist,

15 b) mit der Dienstanforderungsnachricht wird von dem ersten Rechner die Erbringung eines Dienstes angefordert,

c) der zweite Rechner überprüft, ob das in der Dienstanforderungsnachricht enthaltene Paßwort für den ersten Rechner gültig ist,

20 d) für den Fall, daß das Paßwort gültig ist, der Dienst erbracht wird,

e) für den Fall, daß das Paßwort ungültig ist, von dem zweiten Rechner eine Aktualisierungsnachricht an den ersten Rechner gesendet wird, mit der eine Aktualisierung des Paßworts gefordert wird, und

25 f) von dem ersten Rechner ein aktualisiertes Paßwort gebildet wird, welches im weiteren im Rahmen der Kommunikationsverbindung als Paßwort verwendet wird.

Ermittlung des Paßworts

FIG 1

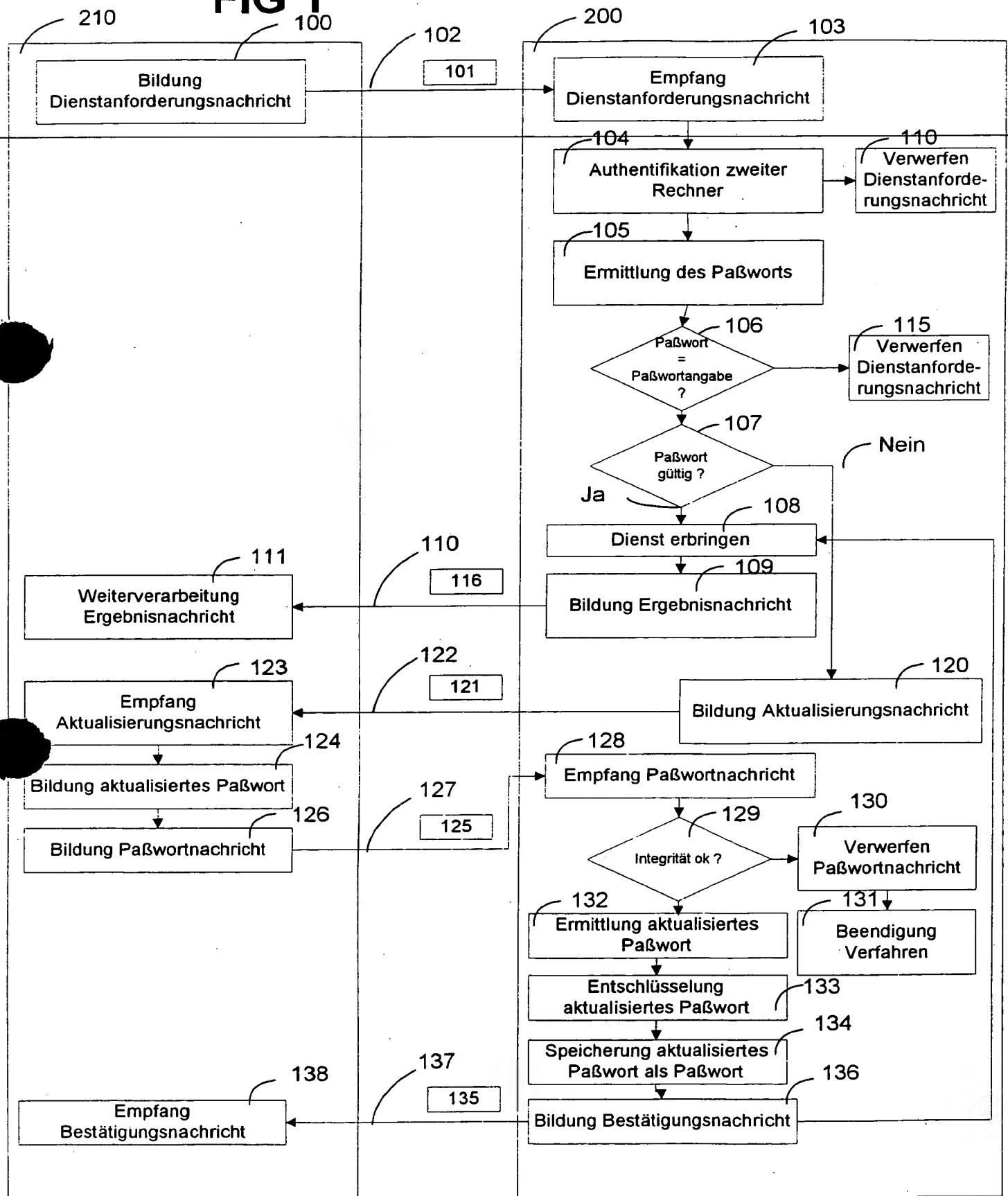


FIG 2

